CLAIMS:

What is claimed is:

1. A method of logging audit events in a data processing system, the method comprising the computer implemented steps of:

writing a sequence of audit records including a final audit record to a first log file stored by a data processing system;

calculating a respective first hash value of each audit record;

responsive to calculating each respective first hash value, calculating a corresponding second hash value from the first hash value and a value of a register associated with the data processing system;

writing the second hash value to the register;

responsive to closing the first log file, opening a second log file; and

writing, to a first record of the second log file, a final second hash value corresponding to a first hash value of the final audit record.

2. The method of claim 1, further comprising:

generating a cryptographically signed value of the final second hash value; and

writing the signed value to the first record of the second log file.

3. The method of claim 2, wherein the signed value is generated using an identity of a trusted platform module of the data processing system.

4. The method of claim 1, wherein each respective first hash value and corresponding second hash value are calculated from a US secure hashing algorithm-1.

5. The method of claim 1, wherein writing the second hash value further comprises:

performing an extend function, wherein the first hash value is included as an operand of an extend function call and the register is a platform configuration register.

6. The method of claim 1, wherein calculating a corresponding second hash further comprises:

concatenating the register value with the first hash value; and

calculating the second hash value from a result of concatenating the register value with the first hash value.

7. A method for verifying a source of a log file, the method comprising the computer implemented steps of:

iteratively calculating a respective first hash value of a plurality of records of a first log file;

responsive to calculating the respective first hash value, calculating a corresponding second hash value from the first hash value and a second value;

responsive to calculating each second hash value, storing the second hash value as the second value;

responsive to calculating a first hash value and a corresponding second hash value for a final record of the plurality of records, comparing the second hash value of the final record to a value stored in a record of a second log file.

8. The method of claim 7, wherein iteratively calculating further comprises:

calculating an initial first hash value, wherein the second value is a stored value of a register read when the first log file is created.

9. The method of claim 7, further comprising:

reading a first record of the first log file, wherein the first record includes an initial value of the second value.

10. A computer program product in a computer readable medium for recording audit events, the computer program product comprising:

first instructions for writing a first sequence of records to a first log file and for writing a second sequence of records to a second log file, wherein the records of the first sequence include a final record;

second instructions for calculating a respective first hash value of each record of the first sequence;

third instructions for calculating a second hash value from the first hash value of the final record, wherein the second hash value is calculated from a hash of the first hash value of the final record and a value of a register; and

fourth instructions for writing the second hash value of the final record to a record of the second log file.

11. The computer program product of claim 10, wherein the first instructions open the second log file upon closing the first log file.

12. The computer program product of claim 11, wherein the third instructions read the value of the register when the first log file is closed.

13. The computer program product of claim 10, wherein the fourth instructions write a cryptographically signed value of the value of the register to the record of the second log file.

14. The computer program product of claim 10, wherein the third instructions calculated a respective second hash value for each first hash value.

15. The computer program product of claim 14, wherein the third instructions write the second hash value to the register upon calculating the respective second hash value for each first hash value.

16. A data processing system for recording audit events, comprising:

a memory that contains a first audit log file and an auditing application as a set of instructions;

a trusted platform module having a platform configuration register; and

a processing unit, responsive to execution of the set of instructions, for calculating a hash value of an audit record written to the first audit log file and that extends a value of the platform configuration register with the hash value, wherein the processing unit, responsive to closing the first log file, identifies a final value of the platform configuration register and writes the final value to a second audit log file.

17. The data processing system of claim 16, wherein the final value is derived from a hash value calculated from a final audit record written to the first audit log file and a value of the platform configuration register identified after writing the final audit record.

18. The data processing system of claim 16, wherein the processing unit calculates a signature of the final value and writes the signature to the second audit log file.

19. The data processing system of claim 16, wherein the signature is generated from an attestation identity key of the trusted platform module.

20. The data processing system of claim 16, wherein the processing unit writes a final audit record to the first audit log file and an audit record generated subsequent to the final audit record to the second audit log file.